AMENDMENTS TO THE CLAIMS

Claims Pending:

- At time of the Action: Claims 1, 2, 5, 6, 9, 10, and 13-63
- Amended Claims: Claims 9, 13, 30, and 47
- Cancelled Claims: Claims 16, 33, and 50
- After this Response: Claims 1, 2, 5, 6, 9, 10, 13-15, 17-32, 34-46, and 48-63

This listing of claims will replace all prior versions and listings, of claims in the application.

1. (Previously Presented) A method comprising:

determining at least one Squared Tate pairing for at least one hyperelliptic curve;

wherein determining the Squared Tate pairing further includes:

forming a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of the hyperelliptic curve C;

wherein the mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain;

cryptographically processing selected information based on the determined Squared Tate pairing;

outputting validation of selected information based on the determined Squared Tate pairing; and

determining a course of action in response to validation of selected information.

2. (Currently Amended) The method as recited in Claim 1, wherein the Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K.

3.-4. (Cancelled).

5. (Previously Presented) A computer storage medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

calculating at least one Squared Tate pairing for at least one hyperelliptic curve;

wherein determining the Squared Tate pairing further includes:

forming a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of the hyperelliptic curve C;

wherein the mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain;

cryptographically processing selected information based on the determined Squared Tate pairing;

outputting validation of selected information based on the determined Squared Tate pairing; and

determining a course of action in response to validation of selected information.

6. (Previously Presented) The computer storage medium as recited in Claim 5, wherein the Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K.

7.-8. (Cancelled).

9. (Currently Amended) An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

logic operatively coupled to the memory and configured to calculate at least one Squared Tate pairing for at least one hyperelliptic curve, and at least partially support cryptographic processing of selected stored information based on the determined Squared Tate pairing;

wherein the logic is further configured to form a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of the hyperelliptic curve C;

wherein the mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain;

determining a hyperelliptic curve C of genus g over a field K, determining a Jacobian $J(C)$ of the hyperelliptic curve C;

a display device coupled to the logic for outputting validation of selected information; and

the logic determining a course of action in response to validation.

10. (Previously Presented) The apparatus as recited in Claim 9, wherein the Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K.

11.-12. (Cancelled).

13. (Currently Amended) A method comprising:

determining a hyperelliptic curve C of genus g over a field K and a positive integer m;

determining a Jacobian $J(C)$ of the hyperelliptic curve C, and wherein each element D of $J(C)$ contains a representative of the form $A - g(P_0)$, where A is an effective divisor of degree g; ~~and~~

determining a plurality of functions $h_{j,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate v_m which is a Squared Tate pairing;

outputting validation of selected information based on the Squared Tate pairing; and

determining a course of action in response to validation of selected information[.] ;

wherein if $P=(x, y)$ is a point on the hyperelliptic curve C, then $-P$ denotes a point $-P:=(x, -y)$, and wherein if a point $P=(x, y)$ occurs in A and $y \neq 0$, then $-P := (x,-y)$ does not occur in A and a representative for identity will be $g(P_0)$.

14. (Currently Amended) The method as recited in Claim 13, wherein ~~said~~ the hyperelliptic curve C is over a field not of characteristic 2.

15. (Original) The method as recited in Claim 13, wherein

for at least one element D of $J(C)$, a representative for iD will be $A_i - g(P_0)$, where A_i is effective of degree g.

16. (Cancelled).

17. (Original) The method as recited in Claim 16, further comprising:

to a representative A_i, associating two polynomials (a_i, b_i) which represent a divisor.

18. (Original) The method as recited in Claim 16, further comprising:

determining D as an m-torsion element of $J(C)$.

19. (Original) The method as recited in Claim 18, further comprising:

if j is an integer, then $h_{j,D} = h_{j,D}(X)$ denoting a rational function on C with divisor $(h_{j,D}) = jA_1 - A_j - ((j-1)\, g)\, (P_0)$.

20. (Original) The method as recited in Claim 18, wherein D is an m-torsion divisor and $A_m = g(P_0)$, and a divisor of $h_{m,D}$ is $(h_{m,D}) = mA_1 - mg(P_0)$.

21 (Original) The method as recited in Claim 18, wherein $h_{m,D}$ is well-defined up to a multiplicative constant.

22. (Previously Presented) The method as recited in Claim 18, further comprising:

evaluating $h_{m,D}$ at a degree zero divisor E on the hyperelliptic curve C, wherein E does not contain $\boldsymbol{P}_0$ and E is prime to A_i.

23. (Original) The method as recited in Claim 18, wherein E is prime to A_i for all i in an addition-subtraction chain for m.

24. (Original) The method as recited in Claim 22, wherein given A_i, A_j, and A_{i+j}, further comprising determining a function $u_{i,j}$ such that a divisor of $u_{i,j}$ is $(u_{i,j}) = A_i + A_j - A_{i+j} - g(P_0)$.

25. (Original) The method as recited in Claim 22, further comprising:

evaluating $h_{j,D}(E)$ such that when j=1, $h_{1,D}$ is 1.

26. (Original) The method as recited in Claim 22, further comprising:

given A_i, A_j, $h_{i,D}(E)$ and $h_{j,D}(E)$, evaluating $u_{i,j}$ to be $(u_{i,j})=A_i + A_j - A_{i+j} - g(P_0)$, and $h_{i+j,D}(E)= h_{i,D}(E)\, h_{j,D}(E)\, u_{i,j}\,(E)$.

27. (Original) The method as recited in Claim 13, further comprising:

determining a function $(u_{i,j}) = A_i + A_j - A_{i+j} - g(P_0)$.

28. (Original) The method as recited in Claim 27, wherein $g = 2$ and $(u_{i,j}) = A_i + A_j - A_{i+j} - 2(P_0)$ is determined as follows

$u_{i,j}(\boldsymbol{X}) := \frac{a_{\text{new}}(x(\boldsymbol{X}))}{b_{\text{new}}(x(\boldsymbol{X})) + y(\boldsymbol{X})} * d(x(X))$, if the degree of a_{new} is greater than 2, otherwise, $u_{i,j}$ is determined as $u_{i,j}(X) := d(x(X))$, wherein $d(x)$ is the greatest common divisor of three polynomials $(a_i(x), a_j(x), b_i(x)+b_j(x))$.

29. (Original) The method as recited in Claim 13, further comprising:

determining a Squared Tate pairing for a hyperelliptic curves v_m, for an m-torsion element D of a Jacobian $J(C)$ and an element E of $J(C)$, with representatives $(P_1)+(P_2)+\ldots+(P_g) - g(P_0)$ and $(Q_1)+(Q_2)+\ldots+(Q_g) - g(P_0)$, respectively, with each P_i and each Q_j on the curve C, with P_i not equal to $\pm Q_j$ for all i, j, determining that

$$v_m(D,E) := (h_{m,D}((\boldsymbol{Q}_1)-(\boldsymbol{-Q}_1)+(\boldsymbol{Q}_2)-(\boldsymbol{-Q}_2)+\ldots+(\boldsymbol{Q}_g)-(\boldsymbol{-Q}_g))^{\frac{q-1}{m}}.$$

30. (Currently Amended) A computer storage medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a hyperelliptic curve C of genus g over a field K and a positive integer m;

determining a Jacobian $J(C)$ of the hyperelliptic curve C, and wherein each element

D of $J(C)$ contains a representative of the form $A - g(P_0)$, where A is an effective divisor of degree g; and

determining a plurality of functions $h_{j,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate v_m which is a Squared Tate pairing;

outputting validation of selected information based on the Squared Tate pairing; and

determining a course of action in response to validation of selected information [.] ;

wherein if $P=(x, y)$ is a point on the hyperelliptic curve C, then $-P$ denotes a point $-P:=(x, -y)$, and wherein if a point $P=(x, y)$ occurs in A and $y \neq 0$, then $-P := (x,-y)$ does not occur in A and a representative for identity will be $g(P_0)$.

31. (Previously Presented) The computer storage medium as recited in Claim 30, wherein the hyperelliptic curve C is not of characteristic 2.

32. (Previously Presented) The computer storage medium as recited in Claim 30, wherein

for at least one element D of $J(C)$, a representative for iD will be $A_i - g(P_0)$, where A_i is effective of degree g.

33. (Cancelled).

34. (Previously Presented) The computer storage medium as recited in Claim 33, further comprising:

to a representative A_i, associating two polynomials (a_i, b_i) which represent a divisor.

35. (Previously Presented) The computer storage medium as recited in Claim 33, further comprising:

determining D as an m-torsion element of $J(C)$.

36. (Previously Presented) The computer storage medium as recited in Claim 35, further comprising:

if j is an integer, then $h_{j,D} = h_{j,D}(X)$ denoting a rational function on C with divisor $(h_{j,D}) = jA_1 - A_j - ((j-1)\, g)\, (P_0)$.

37. (Previously Presented) The computer storage medium as recited in Claim 35, wherein D is an m-torsion divisor and $A_m = g(P_0)$, and a divisor of $h_{m,D}$ is $(h_{m,D}) = mA_1 - mg(P_0)$.

38 (Previously Presented) The computer storage medium as recited in Claim 35, wherein $h_{m,D}$ is well-defined up to a multiplicative constant.

39. (Previously Presented) The computer storage medium as recited in Claim 35, further comprising:

evaluating $h_{m,D}$ at a degree zero divisor E on the hyperelliptic curve C, wherein E does not contain P_0 and E is prime to A_i.

40. (Previously Presented) The computer storage medium as recited in Claim 35, wherein E is prime to A_i for all i in an addition-subtraction chain for m.

41. (Previously Presented) The computer storage medium as recited in Claim 39, wherein given A_i, A_j, and A_{i+j}, further comprising determining a function $u_{i,j}$ such that a divisor of $u_{i,j}$ is $(u_{i,j}) = A_i + A_j - A_{i+j} - g(P_0)$.

42. (Previously Presented) The computer storage medium as recited in Claim 39, further comprising:

evaluating $h_{j,D}(E)$ such that when j=1, $h_{1,D}$ is 1.

43. (Previously Presented) The computer storage medium as recited in Claim 39, further comprising:

given A_i, A_j, $h_{i,D}(E)$ and $h_{j,D}(E)$, evaluating $u_{i,j}$ to be $(u_{i,j})=A_i + A_j - A_{i+j} - g(P_0)$,, and $h_{i+j,D}(E)= h_{i,D}(E)\, h_{j,D}(E)\, u_{i,j}\,(E)$.

44. (Previously Presented) The computer storage medium as recited in Claim 30, further comprising:

determining a function $(u_{i,j}) = A_i + A_j - A_{i+j} - g(P_0)$.

45. (Previously Presented) The computer storage medium as recited in Claim 44, wherein $g = 2$ and

$(u_{i,j}) = A_i + A_j - A_{i+j} - 2(P_0)$ is determined as follows

$$u_{i,j}(\boldsymbol{X}) := \frac{a_{\text{new}}(x(\boldsymbol{X}))}{b_{\text{new}}(x(\boldsymbol{X})) + y(\boldsymbol{X})} * d(x(X)) \text{ , if the degree of } a_{\text{new}} \text{ is}$$

greater than 2, otherwise, $u_{i,j}$ is determined as $u_{i,j}(X) := d(x(X))$, wherein $d(x)$ is the greatest common divisor of three polynomials $(a_i(x), a_j(x), b_i(x)+b_j(x))$.

46. (Previously Presented) The computer storage medium as recited in Claim 30, further comprising:

determining a Squared Tate pairing for a hyperelliptic curves v_m, for an m-torsion element D of a Jacobian $J(C)$ and an element E of $J(C)$, with representatives $(P_1)+(P_2)+\ldots+(P_g) - g(P_0)$ and $(Q_1)+(Q_2)+\ldots+(Q_g) - g(P_0)$, respectively, with each P_i and each Q_j on the curve C, with P_i not equal to $\pm Q_j$ for all i, j, determining that

$$v_m(D,E) := \left(h_{m,D}\left((\boldsymbol{Q}_1)-(\boldsymbol{-Q}_1)+(\boldsymbol{Q}_2)-(\boldsymbol{-Q}_2)+\ldots+(\boldsymbol{Q}_g)-(\boldsymbol{-Q}_g)\right)\right)^{\frac{q-1}{m}}.$$

47. (Currently Amended) An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process; and

logic operatively coupled to the memory and configured to determine a hyperelliptic curve C of genus g over a field K and a positive integer m, determine a Jacobian $J(C)$ of the hyperelliptic curve C, wherein each element D of $J(C)$ contains a representative of the form $A - g(P_0)$ and A is an effective divisor of degree g, and determine a plurality of functions $h_{j,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate v_m which is a Squared Tate pairing;

a display device coupled to the logic for outputting validation of selected information; and

the logic determining a course of action in response to the validation[.] ;

wherein if $P=(x, y)$ is a point on the hyperelliptic curve C, then $-P$ denotes a point $-P:=(x, -y)$, and wherein if a point $P=(x, y)$ occurs in A and $y \neq 0$, then $-P := (x,-y)$ does not occur in A and a representative for identity will be $g(P_0)$.

48. (Previously Presented) The apparatus as recited in Claim 47, wherein the hyperelliptic curve C is not of characteristic 2.

49. (Original) The apparatus as recited in Claim 47, wherein

for at least one element D of $J(C)$, a representative for iD will be $A_i - g(P_0)$, where A_i is effective of degree g.

50. (Cancelled).

51. (Previously Presented) The apparatus as recited in Claim 50, wherein the logic is further configured to, for a representative A_i, associate two polynomials (a_i, b_i) which represent a divisor.

52. (Previously Presented) The apparatus as recited in Claim 50, wherein the logic is further configured to determine D as an m-torsion element of $J(C)$.

53. (Previously Presented) The apparatus as recited in Claim 52, wherein the logic is further configured to, if j is an integer, then determine $h_{j,D} = h_{j,D}(X)$ by denoting a rational function on C with divisor $(h_{j,D}) = jA_1 - A_j - ((j-1)\, g)\, (P_0)$.

54. (Previously Presented) The apparatus as recited in Claim 52, wherein D is an m-torsion divisor and $A_m = g(P_0)$, and a divisor of $h_{m,D}$ is $(h_{m,D}) = mA_1 - mg(P_0)$.

55 (Original) The apparatus as recited in Claim 52, wherein $h_{m,D}$ is well-defined up to a multiplicative constant.

56. (Previously Presented) The apparatus as recited in Claim 52, wherein the logic is further configured to evaluate $h_{m,D}$ at a degree zero divisor E on the hyperelliptic curve C, wherein E does not contain $\boldsymbol{P}_0$ and E is prime to A_i.

57. (Original) The apparatus as recited in Claim 52, wherein E is prime to A_i for all i in an addition-subtraction chain for m.

58. (Previously Presented) The apparatus as recited in Claim 56, wherein given A_i, A_j, and A_{i+j}, and wherein the logic is further configured to determine a function $u_{i,j}$ such that a divisor of $u_{i,j}$ is $(u_{i,j}) = A_i + A_j - A_{i+j} - g(P_0)$.

59. (Previously Presented) The apparatus as recited in Claim 56, wherein the logic is further configured to evaluate $h_{j,D}(E)$ such that when j=1, $h_{1,D}$ is 1.

60. (Previously Presented) The apparatus as recited in Claim 56, wherein the logic is further configured to, given A_i, A_j, $h_{i,D}(E)$ and $h_{j,D}(E)$, evaluate $u_{i,j}$ to be $(u_{i,j})=A_i + A_j - A_{i+j} - g(P_0)$,, and $h_{i+j,D}(E)= h_{i,D}(E)\ h_{j,D}(E)\ u_{i,j}\ (E)$.

61. (Previously Presented) The apparatus as recited in Claim 47, wherein the logic is further configured to determine a function $(u_{i,j}) = A_i + A_j - A_{i+j} - g(P_0)$.

62. (Previously Presented) The apparatus as recited in Claim 61, wherein $g = 2$ and

$(u_{i,j}) = A_i + A_j - A_{i+j} - 2(P_0)$ is determined by the logic as follows

$$u_{i,j}(\boldsymbol{X}) := \frac{a_{\text{new}}\left(x(\boldsymbol{X})\right)}{b_{\text{new}}\left(x(\boldsymbol{X})\right) + y(\boldsymbol{X})} * d(x(X))$$, if the degree of a_{new} is

greater than 2, otherwise, $u_{i,j}$ is determined as $u_{i,j}\ (X) := d(x(X))$, wherein $d(x)$ is the greatest common divisor of three polynomials $(a_i(x),\ a_j(x),\ b_i(x)+b_j(x))$.

63. (Previously Presented) The apparatus as recited in Claim 47, wherein the logic is further configured to determine a Squared Tate pairing for a hyperelliptic curves v_m, for an m-torsion element D of a Jacobian $J(C)$ and an element E of $J(C)$, with representatives $(P_1)+(P_2)+\ldots+(P_g) - g(P_0)$ and $(Q_1)+(Q_2)+\ldots+(Q_g) - g(P_0)$, respectively, with each P_i and each Q_j on the curve C, with P_i not equal to $\pm Q_j$ for all i, j, and to determine that

$$v_m(D,E) := \left(h_{m,D}\left((\boldsymbol{Q}_1)-(\boldsymbol{-Q}_1)+(\boldsymbol{Q}_2)-(\boldsymbol{-Q}_2)+\ldots+(\boldsymbol{Q}_g)-(\boldsymbol{-Q}_g)\right)\right)^{\frac{q-1}{m}}.$$